PRIVACY 101: Orientation Training for all Military Members, Civilian Employees, and Contractor Personnel

What is the Privacy Act (PA)?

- The Privacy Act is an Act to limit an agency's collection and sharing of personal data. The Privacy Act requires that all Executive Branch Agencies follow certain procedures when:

  - Collecting personal information
  - Creating databases containing personal identifiers
  - Maintaining databases containing personal identifiers
  - Disseminating information containing personal data

What are some examples of Privacy Data?

- **Personal data about individuals, such as:**
  - **Financial, credit, and medical data**
  - **Security clearance level**
  - **Leave balances; types of leave used**
  - **Home address and telephone numbers (including home web addresses)**
  - **Social Security Number**
  - **Mother's maiden name; other names used**
  - **Drug test results and the fact of participation in rehabilitation programs**
  - **Family data**
  - **Religion, race, national origin**
  - **Performance ratings**
  - **Names of employees who hold government-issued travel cards, including card data**

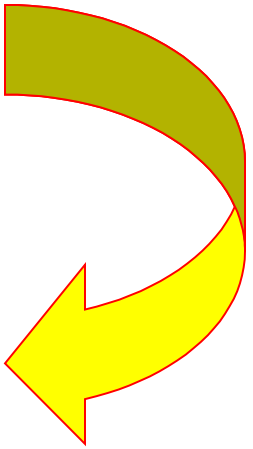
What are the limitations of the Privacy Act?

The Privacy Act applies only to:

US citizens

or

Lawfully admitted aliens



Whose records are filed in a "System of Records" where those records are retrieved by a personal identifier.

What is a System of Records?

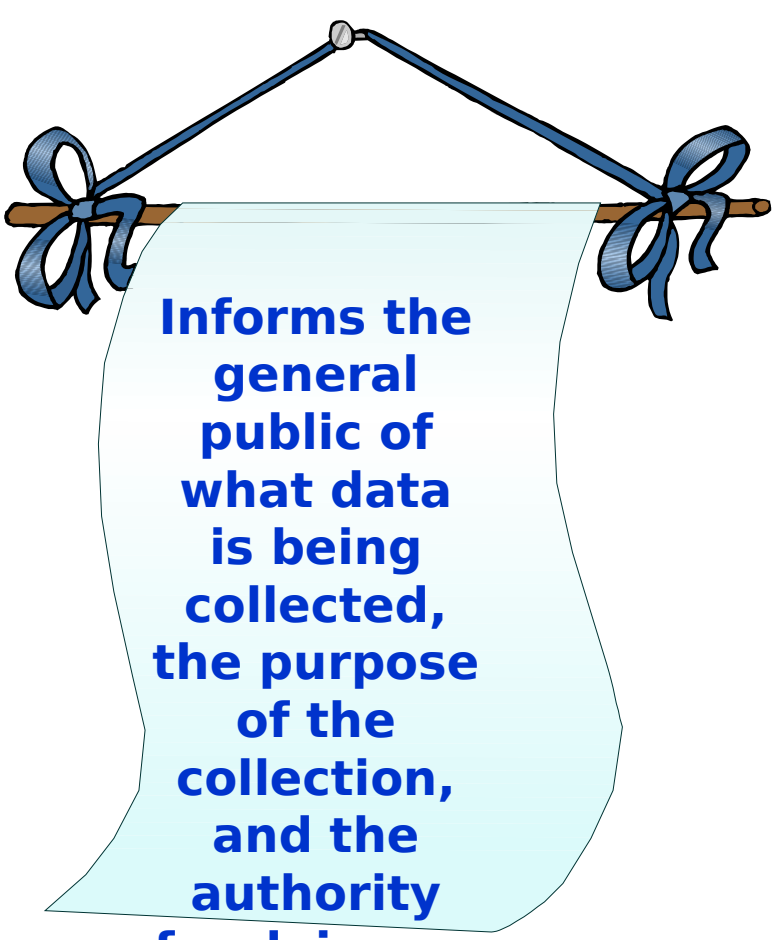
- **A System of Records is a group of records that:**
  - **Contains a personal identifier (such as a name, Social Security Number, Employee Number, etc)**
  - **Contains one other item of personal data (such as home address, performance rating, blood type, etc)**
  - **Is retrieved by a personal identifier**

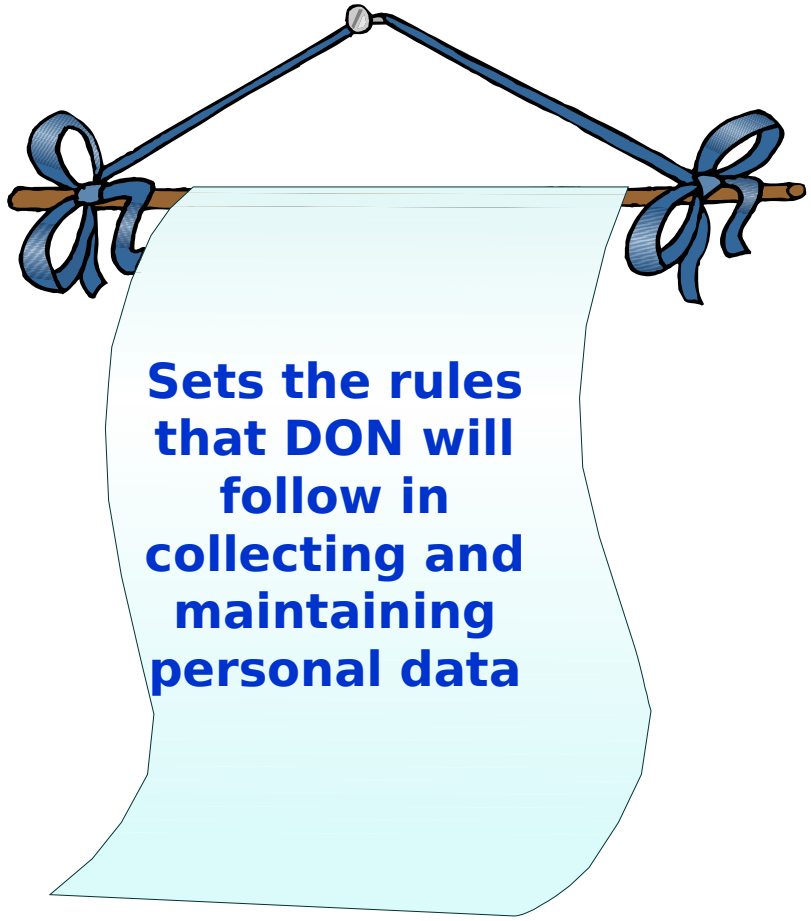
OVERVIEW OF PA SYSTEMS OF RECORDS

- The DON has over 150 PA systems of records. Many systems may be used by any activity, such as correspondence files, recall rosters, badge and credentialing records, etc
- We also maintain systems of records that are unique to a specific activity, such as the Naval Academy, Naval Criminal Investigative Command, Navy Exchange Command, etc
- We also use government-wide systems of records such as under OPM, Dept of Labor, EEOC, etc

What purpose does the System Notice serve?

- **A System Notice:**





PA System Notice

- **Contains the following information:**
  - **System Number:** **We identify Navy systems with "N", Marine Corps systems with "M" and Navy/Marine Corps systems with "NM". The number following is based on the Standard Subject Identification Code (SSIC)**
  - **System location:** **Tells where the files are located**
  - **Categories of individuals covered by the system:** **Tells what people are covered**
  - **Categories of records in the system: Tells what data elements are collected**
  - **Authority for maintenance of the system:**

PA System Notice

- **Policies and practices for storing, retrieving, processing, retaining, and disposing of records contained in the system:**
- **Storage: States whether files are in paper or electronic form**
- **Retrievability: Lists the information that is needed to retrieve a file (such as SSN)**
- **Safeguards: Describes the protections established to safeguard the records**
- **Retention and Disposal: Tells how long the records are kept before they are destroyed**

PA System Notice

- **System manager(s) and address: Gives us the physical address of the manager of record for the system**
- **Notification procedures: Tells how you can learn if you are in the system**
- **Record access procedures: Tells what steps you must take to see your own record**
- **Contesting record procedures: Tells what steps you must take to correct errors in your file**
- **Record source categories: Tells who provided the information**
- **Exemptions Claimed for the System: States whether DON has claimed a PA exemption for this system**

DON PA RESPONSIBILITIES

- Establish rules of conduct for collecting, maintaining, and distributing personal information
- Publish PA system of records notice in the Federal Register
- Collect only data that is authorized by law
- Share data with only those individuals having an official need-to-know

DON PA RESPONSIBILITIES

- Establish and apply data safeguards
- Allow individuals to review records about themselves
- Allow individuals to amend their personal records regarding factual information that is in error
- Keep a record of disclosures made outside of DOD to authorized routine users described in the PA system notice

DON PA RESPONSIBILITIES

- Upon written request, provide a copy of the record upon request to the subject of the file
- Maintain only accurate, timely, and complete information
- When directly soliciting personal information, provide a PA statement that addresses the authority for the collection, purpose for the collection, routine uses that will be made of the information, and whether collection is voluntary or mandatory

DON PA RESPONSIBILITIES

- Follow the guidance set forth in the PA systems notice regarding release/withholding of information
- With some exceptions provided for in the PA, make no disclosure of information without the record subject’s written consent
- When contracts are awarded that involve PA data, ensure the contract contains the appropriate Federal Acquisition Regulation (FAR) privacy clauses

WHAT ARE YOUR RESPONSIBILITIES???

- As an employee, you play a very important role in assuring DON complies with the provisions of the Privacy Act. Accordingly,
  - DO NOT collect personal data without authorization
  - DO NOT distribute or release personal information to other employees unless you are convinced they have an official need-to-know

WHAT ARE YOUR RESPONSIBILITIES???

- DO NOT be afraid to challenge “anyone” who asks to see PA information for which you are responsible
- DO NOT maintain records longer than permitted
- DO NOT destroy records before disposal requirements are met
- DO NOT place unauthorized documents in PA systems of records

WHAT ARE YOUR RESPONSIBILITIES???

- DO NOT commingle information about different individuals in the same file
- DO NOT transmit personal data without ensuring it is properly marked. Use ‘FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE’
- DO NOT use interoffice envelopes to mail Privacy data
- DO NOT place privacy data on shared drives, multi-access calendars, the Intranet or Internet

WHAT ARE YOUR RESPONSIBILITIES???

- DO NOT create a new system of records without first consulting your Privacy Officer
- DO NOT hesitate to offer recommendations on how to better effectively manage privacy data

YOUR INSIGHT COUNTS!!! YOU DEDICATION TO PROTECTING PRIVACY IS PARAMOUNT TO OUR SUCCESS!!!

CONTRACTORS

- AS WE MOVE INTO A BLENDED WORKFORCE, WE MUST ENSURE THAT OUR CONTRACTORS UNDERSTAND THAT THEY TOO MUST COMPLY WITH OUR PRIVACY PROGRAM AND FOLLOW THE SAME RULES AS IF THEY WERE A GOVERNMENT EMPLOYEE

PENALTIES

- There are criminal penalties addressed in the Privacy Act. They are based on knowing and willfully:
  - Obtaining records under false pretenses
  - Disclosing privacy data to any person not entitled to access
  - Maintaining a system of records without meeting public notice requirements
- Result: Misdemeanor criminal charge and a fine of up to $5000

PENALTIES

- Courts may also award civil penalties for:
  - Unlawfully refusing to amend a record
  - Unlawfully refusing to grant access to a record
  - Failure to maintain accurate, relevant, timely, and complete information
  - Failure to comply with any PA provision or agency rule that results in an adverse effect on the subject of the record

PENALTIES FOR THESE VIOLATIONS INCLUDE:

Actual damages

Payment of reasonable attorney's fees

Removal from employment

IN THE PROCESS

- Due to the loss and/or compromise of privacy data, OMB and Congress are addressing what other actions can be taken against employees who fail to comply with the provisions of the Privacy Act

How will I know if the data that I handle is Privacy Act protected data?

- **Privacy data should be marked: "For Official Use Only – Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties"**
- **Be aware that privacy data may not always be marked as such. If you have questions about whether data is protected under the Privacy Act, ask your supervisor**

What is the DON Code of Fair Information Principles?

- **In order to assure that any personal information submitted to DON is properly protected, DON has devised a list of principles to be applied when handling personal information. This is referred to as the "Code of Fair Information Principles"**

- **The "Code of Fair Information Principles" is set forth in a list of 10 policies that DON employees will follow when handling personal information.**

- **Any DON employee, military member, or contractor who handles the personal information of others must abide by the principles set forth by the Code.**

The DON Code of Fair Information Principles

1. <u>The Principle of Openness</u>: When we collect personal data from y we will inform you of the intended uses of the data, the disclosures t will be made, the authorities for the collection, and whether the colle is mandatory or voluntary. We will collect no data subject to the Priv unless a Privacy Act system notice has been published in the Federal Register and posted on the and at www.privacy.navy.mil.

2. <u>The Principle of Individual Participation</u>: Unless DON has claimed exemption from the Privacy Act, we will, upon request, grant you acc your records; provide you a list of disclosures made outside the Depa of Defense ; and make corrections to your file, once shown to be in e

3. <u>The Principle of Limited Collection</u>: DON will collect only those pe data elements required to fulfill an official function or mission groun law. Those collections are conducted by lawful and fair means.

The DON Code of Fair Information Principles (cont'd)

4. The Principle of Limited Retention: DON will retain your personal information only as long as necessary to fulfill the purposes for which is collected. Records will be destroyed in accordance with establishe records management principles.

5. The Principle of Data Quality: DON strives to maintain only accu relevant, timely, and complete data about you.

6. The Principle of Limited Internal Use: DON will use your personal only for lawful purposes. Access to your data will be limited to those Department of Defense individuals with an official need for access.

7. The Principle of Disclosure: DON employees and military member zealously guard your personal data to ensure that all disclosures are with your written permission or are made in strict accordance with t Privacy Act.

The DON Code of Fair Information Principles (cont'd)

8. The Principle of Security: Your personal data is protected by app safeguards to ensure security and confidentiality. Electronic syst be periodically reviewed for compliance with the security principl Privacy Act, the Computer Security Act, and related statutes. Elec collections will be accomplished in a safe and secure manner.

9. The Principle of Accountability: DON and our employees, military members, and contractors are subject to civil and criminal penalti certain breaches of Privacy. DON is diligent in sanctioning individ who violate Privacy rules.

10. The Principle of Challenging Compliance: You may challenge DON you believe that DON has failed to comply with these principles, t Privacy Act, or the rules of a system of records notice. Challenges addressed to the person accountable for compliance with this Cod local Navy/Marine Corps Privacy Act manager, CNO (DNS-36), or CMC (ARSF).

THINK PRIVACY

- YOUR ATTENTION TO PRIVACY SERVES EVERYONE!
- FACTOR PRIVACY IN YOUR WORKPLACE
- DEVELOP BEST PRACTICES

- PLEASE DIRECT ANY QUESTIONS TO YOUR PRIVACY OFFICER OR TO DORIS LAMA, CNO (DNS-36), 202-685-6545, DORIS.LAMA@NAVY.MIL